UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/778,623 | 02/06/2001 | Cheuk W. Ko | NA00-12101 | 9616 |

28875 7590 02/08/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

| EXAMINER | |
|---|---|
| CHAI, LONGBIT | |
| **ART UNIT** | **PAPER NUMBER** |
| 2131 | |

DATE MAILED: 02/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/778,623 | KO, CHEUK W. | |
| | Examiner | Art Unit | |
| | Longbit Chai | 2131 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *21 October 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 February 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. Claims 1 – 24 have been presented for examination. Claims 2, 10 and 18 have been canceled; claims 1, 9 and 17 have been amended; and new claims 25 – 27 have been added in an amendment filed 10/21/2004.

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 3 – 4, 9, 11 – 12, 17, 19 – 20 and 25 – 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warrender ("Detection Intrusions Using System Calls: Alternative Data Models", 1999), hereinafter referred to as Warrender, in view of Cohen (Patent Number: 5481650), hereinafter referred to as Cohen, and in view of Valente (Patent Number: 6779120), hereinafter referred to as Valente.

As per claim 1, 9, and 17, Warrender teaches a method for automatically generating a valid behavior specification for use in an intrusion detection system for a computer system, comprising:

automatically constructing the valid behavior specification from the exemplary set of system calls by selecting a set of rules covering valid system calls (Warrender: see for example, Section 5.3 Line 42 – 43: A list of rules is qualified as a behavior specification);

receiving an exemplary set of system calls that includes positive examples of valid system calls, and possibly negative examples of invalid system calls (Warrender: see for example, Section 1.0 Line 2 – 13: "anomalies", i.e. the system calls that violate the rules, is qualified as "invalid system calls" and the corresponding trace of instance is the "negative example").

However, Warrender does not disclose expressly the negative examples of invalid system calls (for those system calls that violate the rule in the specification).

Cohen teaches the negative examples to be included into the training system in addition to the positive examples (Cohen: see for example, Column 2 Line 59 – 67).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Cohen within the system of Warrender because Warrender teaches detecting intrusions using system calls including a rule induction technique (Warrender: see for example, Abstract Line

11) and Cohen teaches (a) a learning systems that learn by formulating sets of rules from input data and desired responses to such data (Cohen: see for example, Column 1 Line 8 – 10), (b) a more efficient and accurate mechanism by making background knowledge to be conveniently expressed as an input with a single formal structure (Cohen: see for example, Column 1 Line 30 – 33 and Column 2 Line 30 – 32).

Warrender in view of Cohen further teaches:

the set of rules covers all positive examples in the exemplary set of system calls without covering negative examples (Cohen: see for example, Column 2 Line 67); and

selecting a rule for the valid behavior specification involves using an objective function that seeks to maximize the number of positive examples covered by the rule (Cohen: see for example, Column 8 Line 25 – 36 and Column 6 Line 10 – 28).

Warrender in view of Cohen does not disclose expressly selecting a rule for the valid behavior specification involves using an objective function that seeks to maximize the number of positive examples covered by the rule while seeking to minimize the number of possible system calls covered by the rule; and the objective function additionally seeks to minimize the number of privileged system calls covered by the rule.

Valente teaches selecting a rule for the valid behavior specification involves using an objective function that seeks to maximize the number of positive

examples covered by the rule while seeking to minimize the number of possible system calls covered by the rule; and the objective function additionally seeks to minimize the number of privileged system calls covered by the rule (Valente: see for example, Column 41 Line 48 – 62: using the policy of deny access to the system as the precedence rule indeed is the way seeking to minimize the number of privileged system calls covered by the rule because otherwise, the system access would be allowed in the first place instead of deny as taught by Valente).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Cohen within the system of Warrender because Warrender teaches detecting intrusions using system calls including a rule induction technique (Warrender: see for example, Abstract Line 11) and Valente teaches a simple intuitive model for expressing and applying security rules by using a sophisticated algorithm for determining the precedence of the policy rules (Valente: see for example, Column 4 Line 39 – 44).

As per claim 7, 15 and 23, Warrender in view of Cohen and Valente teaches the claimed invention as described above (see claim 1, 9 and 17 respectively). Cohen further teaches the set of rules includes at least one Horn clause teaches (Cohen: see for example, Column 2 Line 59 – 63).

As per claim 8, 16 and 24, Warrender in view of Cohen and Valente teaches the claimed invention as described above (see claim 7, 15 and 23

respectively). Warrender in view of Cohen and Valente further teaches selecting a rule for the valid behavior specification involves:

selecting a positive example from the exemplary set of system calls (Warrender: see for example, Section 1.0 Line 2 – 13);

constructing a Horn clause for the positive example by iterating through a subsumption lattice, starting from a most general possible clause and proceeding to a most specific clause for the positive example, and selecting a Horn clause that maximizes the objective function without covering any negative examples; adding the Horn clause to the set of rules in the valid behavior specification; and removing other positive examples covered by the Horn clause from the exemplary set of system calls, so subsequently selected Horn clauses do not have to cover the other positive examples (Cohen: see for example, Figure 3 and Column 2 Line 59 – 67 and Column 3 Line 1 – 7 and Valente: see for example, Column 41 Line 48 – 62 & Column 4 Line 39 – 44: Examiner notes "subsumption lattice" is not specifically defined in the specification and thereby, it is not clear what the Applicant is exactly referred to. According to the definition in "Robotics Glossary Part 2" by William Cox, subsumption lattice / architecture is interpreted as by giving each of the behavior a priority so that higher priority events always will execute first. Valente teaches the precedence of taking the policy rules (Valente: see for example, Column 4 Line 39 – 44) and Cohen teaches the priority of selecting the clause (rule) is based upon the highest information gain first (i.e.

most general) rules (Cohen: see for example, Column 2 Line 59 – 67). See the same rationale of combination applied herein as above in claim 1.

As per claim 25, Warrender in view of Cohen and Valente teaches the claimed invention as described above (see claim 1). Warrender in view of Cohen and Valente further teaches the objective function includes:

$f_h = e_h - (g_h + p_h + c_h)$, Where:

$f_h$ = the generality of clause h;

$g_h$ = the privilege of clause h;

$p_h$ = the length of the clause à; and

$e_h$ = the explanation power (See the same rationale as addressed above in rejecting the claim 1 and 3: Examiner notes the equation presented above does not quantify any effectiveness of each individual parameter (i.e. the generality, the privilege, and the length of the clause) with respect to the explanation power and merely expresses (a) the objective function is characterized by three factors (i.e. the generality, the privilege, and the length of the clause) and the sufficient information gain is depending upon the reduction of the generality, the privilege, and the length of the clause, which is clearly addressed as above in claim 1 and 3).

As per claim 26, Warrender in view of Cohen and Valente teaches the claimed invention as described above (see claim 25). Cohen further teaches the

values $g_h$ and $p_h$ are normalized to range from 1 to the total number of valid traces (Cohen: see for example, Column 7 Line 1).

As per claim 27, Warrender in view of Cohen and Valente teaches the claimed invention as described above (see claim 26). Cohen further teaches the value f is set to favor short, low-privilege, low-generality clauses while explaining examples in many traces (See the same rationale as addressed above in rejecting claim 25).

3. Claims 5 – 6, 13 – 14 and 21 – 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warrender ("Detection Intrusions Using System Calls: Alternative Data Models", 1999), hereinafter referred to as Warrender, in view of Cohen (Patent Number: 5481650), hereinafter referred to as Cohen, and in view of Valente (Patent Number: 6779120), hereinafter referred to as Valente, in view of Hofmeyr ("Intrusion Detection using Sequence of System Calls", 1998), hereinafter referred to as Hofmeyr.

As per claim 5, 13 and 21, Warrender in view of Cohen and Valente teaches the claimed invention as described above (see claim 1, 9 and 17 respectively). Warrender in view of Cohen and Valente does not teach producing the exemplary set of system calls by running an exemplary program and recording system calls generated by the exemplary program.

Hofmeyr teaches producing the exemplary set of system calls by running an exemplary program and recording system calls generated by the exemplary program (Hofmeyr: see for example, Page 3 Line 11 – 14).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Hofmeyr within the system of Warrender because Warrender teaches detecting intrusions using system calls and Hofmeyr teaches detecting intrusions at the level of privileged processes (Hofmeyr: see for example, Abstract).

As per claim 6, 14 and 22, Warrender in view of Cohen and Valente teaches the claimed invention as described above (see claim 1, 9 and 17 respectively). Warrender in view of Cohen and Valente does not teach the exemplary set of system calls includes calls to functions implemented by an operating system of the computer system.

Hofmeyr teaches the exemplary set of system calls includes calls to functions implemented by an operating system of the computer system (Hofmeyr: see for example, Page 11 Line 1 – 2). See same rationale of combination applies here as above in rejecting claim 5.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-

272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100